1. Purpose

- 1.1 LionFinTech Pte. Ltd. (“LionFinTech”, “we”, “our”) is committed to complying with Singapore’s Personal Data Protection Act 2012 (“PDPA”).
- 1.2 This policy establishes how we collect, use, disclose, and safeguard personal data of our customers, employees, and partners.
- 1.3 We adopt a strict AI Usage & Data Privacy Framework to ensure sensitive information is not inadvertently shared with external AI tools, cloud services, or unauthorised parties.

---

2. Scope

2.1 This Policy applies to:

- All employees, contractors, and interns of LionFinTech.
- All forms of personal data handled by LionFinTech, whether in electronic or hardcopy form.
- All interactions with external AI systems (e.g., ChatGPT, GitHub Copilot, third-party SaaS LLMs).

---

3. Categories of Sensitive Data (Prohibited for External Disclosure)

3.1 Personal Identifiers (Protected under PDPA)

- **Clause 3.1.1:** Employees must not disclose NRIC numbers.
  Reason: NRIC numbers can be used for identity theft, fraud, and unauthorised access to personal services.
- **Clause 3.1.2:** Employees must not disclose Foreign Identification Numbers (FIN).
  Reason: FINs can lead to identity-related fraud for foreign staff or clients.
- **Clause 3.1.3:** Employees must not disclose passport numbers.
  Reason: Passport numbers can be misused for identity theft or illegal travel documentation.
- **Clause 3.1.4:** Employees must not disclose contact information (mobile numbers, email addresses, home addresses).

Reason: Exposure can result in phishing attacks, spam, harassment, or social engineering.

3.2 Financial Data

- **Clause 3.2.1:** Employees must not disclose bank account numbers.
  Reason: Can lead to unauthorised transactions or account takeover.

- **Clause 3.2.2:** Employees must not disclose credit card details.
  Reason: Exposed credit card information can be directly used for fraud.

- **Clause 3.2.3:** Employees must not disclose transaction histories.
  Reason: Reveals private spending behavior, potentially enabling social engineering attacks.

- **Clause 3.2.4:** Employees must not disclose salary, bonuses, or compensation details.
  Reason: Exposure risks privacy violations, internal disputes, and reputational damage.

3.3 Authentication & Access Credentials

- **Clause 3.3.1:** Employees must not disclose API keys.
  Reason: Can grant unauthorised access to company or third-party systems.

- **Clause 3.3.2:** Employees must not disclose access tokens.
  Reason: May allow attackers to impersonate employees and extract sensitive data.

- **Clause 3.3.3:** Employees must not disclose passwords.
  Reason: Can compromise both personal and corporate accounts.

- **Clause 3.3.4:** Employees must not disclose encryption keys.
  Reason: Exposure can decrypt confidential files or communications.

- **Clause 3.3.5:** Employees must not disclose source code containing embedded credentials.
  Reason: Could result in intellectual property theft and compromise of internal systems.

3.4 Business Confidential Information

- **Clause 3.4.1:** Employees must not disclose internal project codenames (e.g., “Project LionX”).
  Reason: Disclosure may reveal ongoing initiatives and competitive advantage.

- **Clause 3.4.2:** Employees must not disclose product roadmaps and unreleased features.
  Reason: Exposure can harm market positioning or allow competitors to copy plans.

- **Clause 3.4.3:** Employees must not disclose strategic business or financial plans.
  Reason: Reveals market strategy, potential M&A activities, or revenue plans.

- **Clause 3.4.4:** Employees must not disclose vendor and partner contracts.
  Reason: Breaches confidentiality agreements and damages business relationships.

---

4. Employee Responsibilities

- **Clause 4.1:** Employees must never input or transmit sensitive data into external AI tools.
  Reason: External AI tools are outside LionFinTech's control and may expose data.

- **Clause 4.2:** Obfuscation of sensitive data does not provide protection.
  Reason: AI systems can infer or reconstruct disguised identifiers.

- **Clause 4.3:** Sensitive data must remain within authorised LionFinTech systems.
  Reason: Ensures compliance with PDPA and MAS TRM security standards.

- **Clause 4.4:** Accidental disclosure of sensitive data must be reported immediately to the Data Protection Officer (DPO).
  Reason: Prompt reporting allows mitigation and demonstrates compliance.

---

5. PDPA Compliance Clauses

- **Clause 5.1 (Consent – Section 13):** Personal data must not be disclosed without individual consent.

- **Clause 5.2 (Purpose Limitation – Section 18):** Data must only be used for intended, lawful purposes.

- **Clause 5.3 (Protection Obligation – Section 24):** Organisations must protect personal data from unauthorised access, use, or disclosure.

- **Clause 5.4 (Retention Limitation – Section 25):** Personal data must be deleted when it no longer serves a legal or business purpose.

---

6. Monitoring & AI Compliance Firewall

- **Clause 6.1:** All AI interactions within LionFinTech are monitored in real-time.
- **Clause 6.2:** Prompts sent to external AI systems are automatically scanned by LionFinTech's Policy-Aware AI Privacy Guardian.
- **Clause 6.3:** The system flags, blocks, or masks sensitive data and logs violations per policy clauses.

---

7. Data Protection Officer (DPO)

- **Clause 7.1:** LionFinTech has appointed a DPO to oversee PDPA compliance.
    - Contact: [Insert DPO Name & Email]

---

8. Enforcement & Consequences

- **Clause 8.1:** Non-compliance may result in mandatory retraining on PDPA and internal data privacy.
- **Clause 8.2:** Repeated or serious breaches may lead to disciplinary action, including termination.
- **Clause 8.3:** Breaches may be reported to the Personal Data Protection Commission (PDPC).

---

9. Review & Updates

- **Clause 9.1:** This policy will be reviewed annually or whenever PDPA or MAS guidelines are updated.